RISEBA
UNIVERSITY OF APPLIED SCIENCES
Business I Arts I Technology

Risk Management System

2026

RISEBA Risk Management Policy

1. The RISEBA Risk Management Policy aims to define the fundamental principles, scope and organisation of risk management at RISEBA.

2. Risk management is implemented across all areas of RISEBA's operations, including the setting and achievement of strategic and operational objectives, the introduction of change and innovation, decision-making and the implementation of processes.

3. RISEBA defines risk management as an integral part of strategic management and an element of the internal control system.

4. RISEBA uses risk management to analyse risks and their impact, to manage risks promptly and to protect RISEBA against the impact of significant risks, thereby promoting informed decision-making and the effective use of resources.

5. Risk management is aimed at facilitating the implementation of RISEBA's strategy whilst minimising future losses arising from potential undesirable events.

6. The key principles of risk management implemented by RISEBA are:

    6.1. a risk-based approach;
    6.2. timely response;
    6.3. risk management as a cyclical and continuous process;
    6.4. clarity of responsibilities and authorities;
    6.5. awareness and involvement of staff and stakeholders;
    6.6. risk assessment and decision-making based on data, information and evidence;
    6.7. regular review of the risk management system, learning from experience and continuous improvement.

7. The purpose of risk management is to ensure the identification and assessment of risks at RISEBA, the determination of the likelihood of risks occurring and their potential impact on RISEBA's operations and the achievement of its objectives, as well as the planning, implementation and review of appropriate risk management, control and monitoring measures.

8. As part of the risk identification and assessment process, RISEBA simultaneously identifies opportunities that may contribute to the achievement of strategic and operational objectives, organisational development, innovation, operational efficiency and performance improvement.

9. RISEBA manages risks in the following categories:

    9.1. strategic risks: the economic situation, global trends, political influence, planning errors, damage to reputation, etc.;

    9.2. financial risks: availability of funding, inadequate financial planning, etc.;

9.3. operational risks: staff errors, non-compliance of information technology and information systems, inadequate or incomplete internal processes, risks affecting the working environment and external threats;

9.4. legal/compliance risks: failure to comply with or misinterpretation of regulatory requirements, personal data protection risks, etc.;

9.5. risks of fraud and breaches of ethical standards;

9.6. project risks: risks associated with the submission, implementation and sustainability of projects.

10. RISEBA assesses the impact of risks in terms of their potential effect on the following areas:

    10.1. RISEBA's financial stability and financial performance;

    10.2. the achievement of RISEBA's strategic and operational objectives;

    10.3. RISEBA's reputation;

    10.4. RISEBA's business continuity and the implementation of processes;

    10.5. Compliance with regulatory requirements and internal policies.

11. To ensure a unified and coordinated approach to risk management, the allocation of risk management responsibilities at RISEBA, the stages involved and the methodology used in their implementation are set out in the RISEBA Risk Management Procedure.

RISEBA Risk Management Procedure

1. The RISEBA Risk Management Procedure aims to establish a uniform and coordinated approach to the implementation of risk management at RISEBA, setting out the allocation of responsibilities, the stages of risk management and the methodology used in its implementation.

2. Terminology used in the RISEBA Risk Management Procedure:

   2.1. Risk – the likelihood of an event or events, or circumstances, that may adversely affect the implementation of RISEBA's operations or the achievement of its strategic objectives;

   2.2. Risk management – a systematic management process implemented to minimise future losses caused by potential undesirable events;

   2.3. Risk owner – the head of a structural unit or a person appointed by the Rector within whose area of responsibility a risk may materialise;

   2.4. Risk identification – the process of identifying, recognising and describing risks;

   2.5. Risk event – one or more potential events or circumstances that may affect RISEBA's operations or the achievement of its strategic objectives;

   2.6. Risk incident – a risk event that has already occurred and which causes or may cause adverse consequences for RISEBA's operations or the achievement of its objectives;

   2.7. Risk analysis – the compilation and evaluation of risk-related data, information and accumulated experience, to determine the impact of a risk and the probability of its occurrence;

   2.8. Risk impact – the potential negative consequences of a risk on RISEBA's operations and the achievement of its objectives;

   2.9. Probability of risk – the likelihood of a specific risk materialising within the next year under current circumstances;

   2.10. Risk value – the product of the risk impact and the probability of the risk;

   2.11. Risk level – the magnitude of the risk (assessed according to the risk value), which helps to determine the need for appropriate action;

   2.12. Risk map – a methodological tool for determining the risk level corresponding to the risk value;

   2.13. Risk register – a document accessible to a restricted group, summarising information on identified risks, their assessment, necessary risk management measures, their implementation deadlines and risk owners;

2.14. Risk management report – an annual report by the Rector to the Board on the implementation of RISEBA's risk management system, including the management of high- and very high-risk risks.

3. The distribution of responsibilities and powers amongst those involved in risk management is set out in Figure 1.

STAKEHOLDERS AND THEIR RESPONSIBILITIES IN THE RISK MANAGEMENT SYSTEM

Stakeholder	Responsibilities and authorities
Governing Board	1. Approves the RISEBA Risk Management Policy. 2. Reviews and approves the annual RISEBA Risk Management Report and, where necessary, adopts binding decisions. 3. Evaluates the RISEBA risk management system and its effectiveness.
Rector	1. Ensures the development and periodic review of the RISEBA Risk Management Policy in cooperation with the Management Team. 2. Provides the resources and appropriate authorisations necessary for the establishment, implementation, maintenance and improvement of the risk management system. 3. Approves the Risk Register and ensures the implementation and monitoring of the risk mitigation measures specified therein. 4. Submits the annual RISEBA Risk Management Report to the Governing Board.
Management Team	1. Reviews the identified risks, their assessments and the defined risk mitigation measures, evaluating their adequacy and compliance. 2. Decides on the inclusion of risks in the Risk Register.
Head of Human Resources and Office (Risk Coordinator)	1. Implements, executes and maintains the risk management system. 2. Maintains and monitors the RISEBA Risk Register. 3. Collects and summarises information on initially identified risks, their assessments and possible risk mitigation measures, and submits this for review by the Management Team. 4. Coordinates the work of the Management Team on risk management matters and its cooperation with risk owners. 5. Summarises information on changes in risk assessments and the implementation of risk mitigation measures. 6. Provides advice and support to the RISEBA management and other parties involved in risk management on the implementation of risk management matters. 7. Compiles information for the annual Risk Management Report, prepares its draft and submits and presents it to the Rector.
Risk Owner	1. Conducts risk assessment and defines risk mitigation measures. 2. Implements the risk mitigation measures specified in the RISEBA Risk Register. 3. Monitors and regularly re-evaluates the risks within their area of responsibility on a daily basis.
Head of Structural Unit / Project Manager	1. Identifies risks within their area of responsibility in the risk categories defined in the RISEBA Risk Management Policy, including by collecting information from subordinate employees and/or other relevant stakeholders. 2. Informs the Head of Human Resources and Office about the identified risks, their initial assessment and possible risk mitigation measures, and submits the information to the Management Team.
Employee	1. Timely informs their direct manager about an incident or potential risk in their area of work. 2. Provides the data and information necessary for risk analysis to their direct manager and to the Head of Human Resources and Office.

RISEBA | People Ideas Impact

Managing risks.
Creating opportunities.

Figure 1. Distribution of responsibilities and powers within the RISEBA risk management system.

4. The head of a department or project systematically identifies and records risks within their area of responsibility, taking into account RISEBA's strategic and operational objectives, process outcomes, changes and trends in the internal and external environment, incidents, the results of audits and inspections, as well as information provided by staff and other stakeholders.

5. Each identified risk is assigned to one of the risk categories set out in RISEBA's Risk Management Policy:

    5.1. strategic risks: the economic situation, security risks, global trends, political influence, planning errors, damage to reputation, etc.;

    5.2. Financial risks: availability of funding, inadequate financial planning, etc.;

    5.3. Operational risks: staff errors, non-compliance of information technology and information systems, inadequate or incomplete internal processes, risks affecting the working environment and external threats;

    5.4. Legal/compliance risks: failure to comply with or misinterpretation of regulatory requirements, personal data protection risks, etc.;

    5.5. Risks of fraud and breaches of ethical standards;

    5.6. Project risks: risks associated with project application, implementation, and sustainability.

6. The head of the department or project manager initially assesses each identified risk, drawing on accumulated experience, information obtained from various sources and forecasts, on a five-point scale (Figure 2):

    6.1. by assigning one of the values for the probability of the risk occurring;

    6.2. assigning one of the values for the impact of the risk.

RISEBA RISK ASSESSMENT SCALES

ASSESSMENT OF RISK LIKELIHOOD

NUMERICAL SCORE	DESCRIPTION OF THE SCORE	KEY CHARACTERISTICS	ADDITIONAL INDICATORS
5	Very likely	• Highly likely to occur; • Expected to occur repeatedly within a year.	• A similar incident has been identified at another higher education institution. • No risk mitigation measures have been implemented.
4	Likely	• High probability of occurring within a year.	• A similar event has been identified at another higher education institution. • Some, but limited, risk mitigation measures have been implemented.
3	Possible	• There is a realistic possibility of occurring within a year.	• Significant changes have occurred in the external environment of RISEBA or within RISEBA or one of its organisational units during the last year. • Risk mitigation measures are not considered fully sufficient.
2	Unlikely	• Occurrence is improbable; would require a combination of several circumstances.	• A similar event has been identified at a comparable higher education institution.
1	Very unlikely	• Extremely unlikely to occur.	• RISEBA's operations are relatively stable, and no similar risk has been identified in the last year. • May occur as a result of force majeure.

The assessment is carried out on a 5-point scale, where 1 – lowest level, 5 – highest level.

ASSESSMENT OF RISK IMPACT

NUMERICAL SCORE	DESCRIPTION OF THE SCORE	KEY CHARACTERISTICS
5	Very high	• Significant financial impact. • Failure to achieve strategic objectives. • Major reputational damage. • Significant disruption to business continuity / processes. • Major non-compliance with external or internal regulatory requirements.
4	High	• Impact on financial performance. • Failure to achieve certain strategic objectives. • Public attention or criticism. • Disruption to business continuity / processes. • Non-compliance with external regulatory requirements that affects decision-making.
3	Medium	• Potential financial losses exceeding the acceptable level, including the need for additional activities to rectify errors or deficiencies. • Delays in achieving certain strategic objectives. • Increased public attention or criticism. • Repeated complaints about processes. • Certain non-compliance with regulatory requirements that may hinder decision-making.
2	Low	• Does not hinder the achievement of strategic objectives. • Reputational damage at national level may be minimal. • Isolated customer complaints about formal matters. • Formal breaches of regulatory requirements that do not affect the quality and compliance of operations.
1	Very low	• Negligible impact on the area of operations. • Does not hinder the achievement of operational objectives. • Minor technical inaccuracies in documents. • Does not affect the quality and compliance of operations.

Figure 2. RISEBA risk assessment scales.

7. The risk impact scale is applied to each area separately in accordance with the RISEBA Risk Management Policy, assessing the impact separately on:

    7.1. RISEBA’s financial stability and financial performance;

    7.2. the achievement of RISEBA’s strategic and operational objectives;

    7.3. RISEBA’s reputation;

    7.4. the continuity of RISEBA’s operations and the implementation of its processes;

    7.5. compliance with regulatory requirements and internal standards.

8. A risk value is calculated for each identified risk by multiplying the numerical values of the risk impact and risk probability (Risk value = Impact × Probability). The risk level is determined in accordance with the calculated risk value. If the risk impact is assessed across several impact areas, the overall risk impact assessment is determined by taking the highest of the assessments obtained for the relevant impact areas.

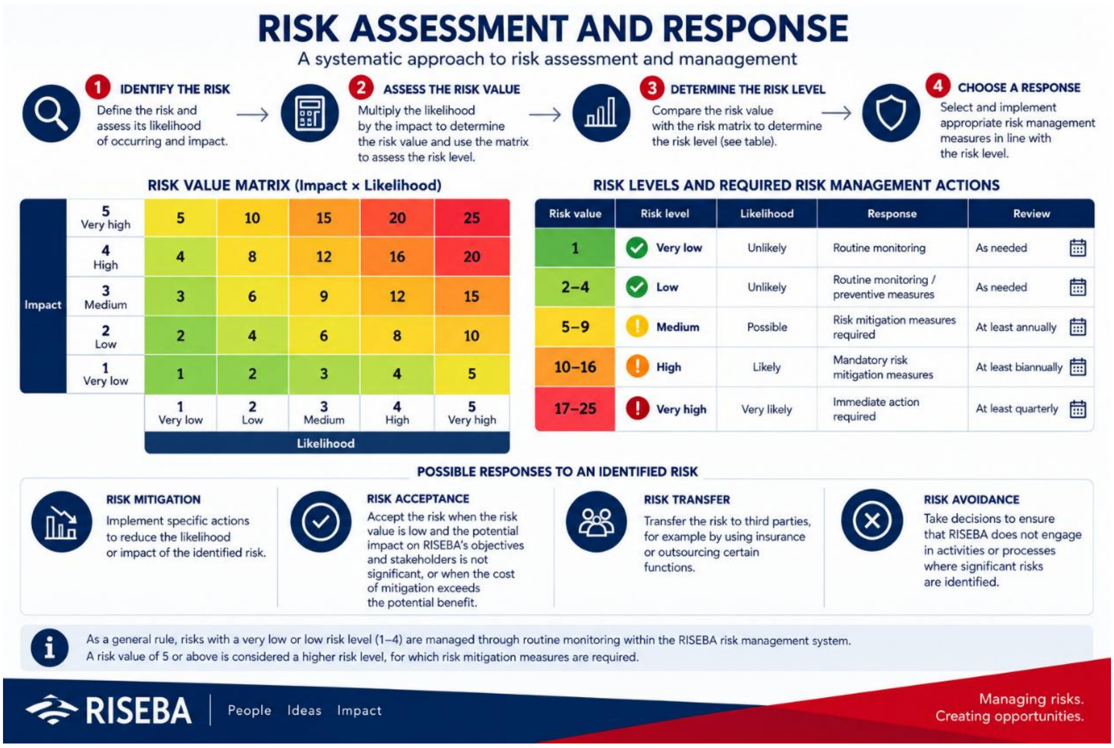

Figure 3. Calculation and level of the RISEBA value.

9. Appropriate risk management measures are selected for each risk, depending on the risk level.

10. In the RISEBA risk management system, a very low or low priority risk level (risk value 1–4) is considered an acceptable risk level. A risk value of 5 or higher is considered a risk level that requires management measures to mitigate it.

11. In relation to the management of identified risks, RISEBA has the following possible courses of action:

11.1. Risk mitigation – specific actions are implemented to mitigate the identified risk;

11.2. Risk acceptance – the risk is accepted by RISEBA's management or the risk owner, and no actions are taken to mitigate it; for example, this approach may be adopted for risks with a low impact and a low probability of occurrence.

11.3. Transfer of risk to third parties – the risk is transferred to third parties, for example, by using the services of an insurance company;

11.4. Risk avoidance – a decision is taken for RISEBA to refrain from carrying out activities or processes in which the identified risk may arise.

12. The head of the department or the project manager submits summarised information on the identified risks and their assessments to RISEBA's Head of Human Resources and Administration, who then forwards it to the Management Group for consideration.

13. If an identified risk or an incident that has occurred may pose a significant or immediate threat to RISEBA's operations, the achievement of its objectives, its financial stability, its reputation or its compliance with regulatory requirements, the immediate line manager and the RISEBA Risk Management Coordinator, as well as other responsible persons in accordance with RISEBA's internal regulatory documents, must be informed without delay.

14. Following a significant risk incident, the risk owner, in collaboration with the risk management coordinator, shall assess the causes and consequences of the incident, the effectiveness of existing control measures, and the need to establish additional risk mitigation measures or improve the relevant processes. The results of the assessment and the lessons learnt from the incident, where applicable, are used to update the Risk Register and improve the risk management system.

15. The Risk Register includes risks whose risk value reaches the materiality threshold set by RISEBA, as well as other risks which the Management Group recognises as material to the achievement of RISEBA's objectives.

16. Once a risk has been included in the Risk Register, the risk owner ensures that the risk assessment is refined, if necessary, and is responsible for defining and implementing risk management measures.

17. The Management Group designates the risk owner and agrees on the risk ratings and the adequacy and appropriateness of risk mitigation measures.

18. The Rector reviews, assesses and approves the RISEBA Risk Register and oversees the implementation of the risk mitigation measures set out therein.

19. Risk owners ensure that the necessary risk mitigation measures are implemented in accordance with the approved RISEBA Risk Register, informing the Head of Human Resources and the Head of Administration of their implementation, including informing the parties involved and the relevant staff of the risks to which they are exposed and the measures to be taken to mitigate these risks.

20. Following the implementation of significant risk mitigation measures, the risk owner reassesses the likelihood and impact of the risk and determines the residual risk, which is recorded in the Risk Register.

21. The Head of Human Resources and Administration coordinates and monitors the implementation of risk mitigation measures by compiling information on the implementation of such measures.

22. Risk monitoring and review are carried out once a year or more frequently (as required) in the case of very high-priority risks:

    22.1. The risk owner individually reviews the risks within their remit and the implementation of risk mitigation measures, and informs the Head of Human Resources and Administration of the results and any changes to the measures, if necessary;

    22.2. The Management Group, when reviewing the RISEBA Risk Register as part of its strategic oversight, including by assessing the information compiled by the Head of Human Resources and the Head of Administration regarding newly identified risks by department or project managers, changes to existing risk assessments, and the results of monitoring the implementation of mitigation measures;

    22.3. As part of the risk review, assess trends in risk changes, the results and effectiveness of the risk mitigation measures implemented, the level of residual risk, new or potential risks, as well as changes in the internal and external environment that may affect the achievement of RISEBA’s strategic and operational objectives.

23. As a result of risk monitoring and review, the RISEBA Risk Register is updated and approved by the Rector.

24. Once a year, as part of the strategic review, the RISEBA Risk Management Review is prepared, on the basis of which the Rector submits the annual RISEBA Risk Management Report to the Board. The report includes information on the most significant and newly identified risks, trends in changes to risk levels, high- and very high-level risks, the implementation and effectiveness of risk mitigation measures, residual risks, significant incidents and the lessons learnt from them, as well as the necessary measures to improve the risk management system.

25. The Head of Human Resources and Administration ensures that the RISEBA Risk Register is accessible to risk owners and other staff designated by the Rector. Upon the recommendation of the Management Group, a decision may be taken regarding the confidentiality of individual risk management elements.

26. The Board evaluates the RISEBA Risk Management System and its effectiveness.

1. Annex – RISEBA Risk Management System

2. Annex – Structure of the RISEBA Risk Register

Risk ID	Risk name and description, including a description of the impact, probability of occurrence, and consequences	Risk category	Scope of impact	Related RISEBA strategic/operational objective or process	Probability of occurrence	Impact	Risk value	Risk-related activities	Description of risk management actions	Deadline for completing actions	Risk owner	Monitoring notes (existing controls / additional measures required)	Residual risk following implementation of measures